PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212462
(43)Date of publication of application : 06.08.1999

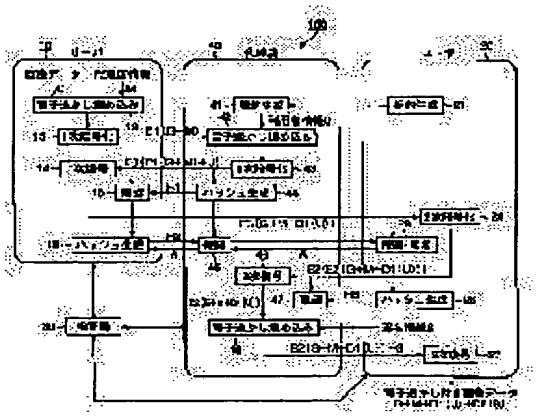
(51)Int.Cl. G09C 5/00
G09C 1/00
H04L 9/32
H04N 1/387
H04N 7/167

(21)Application number : 10-013955
(22)Date of filing : 27.01.1998

(71)Applicant : CANON INC
(72)Inventor : IWAMURA KEIICHI

(54) ELECTRONIC WATERMARK SYSTEM, ELECTRONIC INFORMATION DELIVERY SYSTEM, PICTURE FILING DEVICE, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic information delivery system which surely prevents wrong delivery of data even in the case that elements constituting the purchase and sale of data are hierarchical.
SOLUTION: A first entity 10 subjects original data G to primary encryption processing. A second entity 40 manages and delivers data E1(G+M) after the primary encryption processing and subjects this data to electronic watermark burying processing. A third entity 20 subjects data E3(G+M+D1(U)) after the electronic watermark burying processing to secondary encryption processing.



LEGAL STATUS

[Date of request for examination] 20.05.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－212462

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00	
	1/00	６４０		1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｎ	1/387	
Ｈ０４Ｎ	1/387		Ｈ０４Ｌ	9/00	６７５Ｄ
	7/167		Ｈ０４Ｎ	7/167	Ｚ

審査請求　未請求　請求項の数22　ＯＬ　（全 21 頁）

(21)出願番号　特願平10－13955

(22)出願日　平成10年(1998)１月27日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

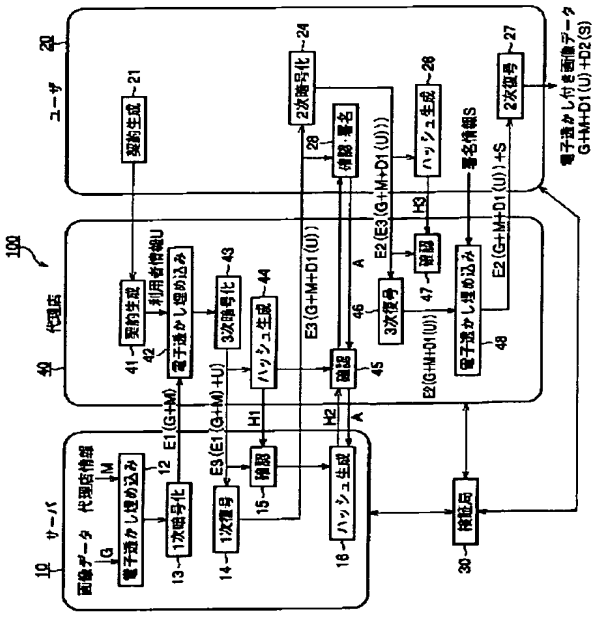
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　電子透かし方式、電子情報配布システム、画像ファイル装置、及び記憶媒体

(57)【要約】

【課題】　データの売買を構成する要素が階層的であっても、データの不正配付を確実に防止する電子情報配布システムを提供する。

【解決手段】　第１のエンティティ１０は、原データＧに１次暗号化処理を行う。第２のエンティティ４０は、１次暗号化処理後のデータＥ１（Ｇ＋Ｍ）を管理及び配布すると共に、それに電子透かし埋込処理を行う。第３のエンティティ２０は、電子透かし埋込処理後のデータＥ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））に２次暗号化処理を行う。



【特許請求の範囲】
【請求項１】　第１のエンティティが原データに１次暗号化処理を行う第１の工程と、
第２のエンティティが上記１次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行うと共に、電子透かし埋込処理を行う第２の工程と、
第３のエンティティが上記電子透かし埋込処理後のデータに２次暗号化処理を行う第３の工程とを含むことを特徴とする電子透かし方式。
【請求項２】　上記第１の工程は、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含むことを特徴とする請求項１記載の電子透かし方式。
【請求項３】　上記第２の工程は、上記電子透かし埋込処理の少なくとも前及び後の何れかに、３次暗号化処理を行う工程を含むことを特徴とする請求項１記載の電子透かし方式。
【請求項４】　少なくとも上記１次暗号化処理及び２次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する工程を更に含むことを特徴とする請求項１記載の電子透かし方式。
【請求項５】　認証局による証明書付き匿名公開鍵によって上記第３のエンティティの署名を検査する工程を更に含むことを特徴とする請求項１記載の電子透かし方式。
【請求項６】　上記第２のエンティティは、複数のエンティティを含むことを特徴とする請求項１記載の電子透かし方式。
【請求項７】　上記第２のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第３のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする請求項１記載の電子透かし方式。
【請求項８】　上記第１の工程は、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含み、
第ｎ（ｎ≧１）のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも第ｎ＋１のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする請求項１記載の電子透かし方式。
【請求項９】　上記電子透かし埋込処理は、少なくとも上記第２のエンティティに関する情報を埋め込まない処理であることを特徴とする請求項１又は２に記載の電子透かし方式。
【請求項１０】　上記原データは、画像データであることを特徴とする請求項１記載の電子透かし方式。
【請求項１１】　少なくとも第１～第３のエンティティを含み、ネットワーク上でのデータの送受信を行う電子情報配布システムであって、
上記第１のエンティティは、原データに１次暗号化処理を行う１次暗号化処理手段を備え、
上記第２のエンティティは、上記１次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行う管理配布処理手段と、電子透かし埋込処理を行う電子透かし埋込処理手段とを備え、
上記第３のエンティティは、上記電子透かし埋込処理後のデータに２次暗号化処理を行う２次暗号化処理手段を備えることを特徴とする電子情報配布システム。
【請求項１２】　上記第１のエンティティは、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備えることを特徴とする請求項１１記載の電子情報配布システム。
【請求項１３】　上記第２のエンティティは、上記電子透かし埋込処理の少なくとも前及び後の何れかに、３次暗号化処理を行う３次暗号化処理手段を更に備えることを特徴とする請求項１１記載の電子情報配布システム。
【請求項１４】　少なくとも上記１次暗号化処理及び２次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する配布手段を更に備えることを特徴とする請求項１１記載の電子情報配布システム。
【請求項１５】　認証局による証明書付き匿名公開鍵によって上記第３のエンティティの署名を検査する検査手段を更に備えることを特徴とする請求項１１記載の電子情報配布システム。
【請求項１６】　上記第２のエンティティは、複数のエンティティを含むことを特徴とする請求項１１記載の電子情報配布システム。
【請求項１７】　上記第２のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第３のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする請求項１１記載の電子情報配布システム。
【請求項１８】　上記第１のエンティティは、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備え、
第ｎ（ｎ≧１）のエンティティの上記電子透かし埋込処理手段は、上記電子透かし埋込処理により埋め込む情報を、少なくとも第ｎ＋１のエンティティに関する情報及び送信するデータに関する情報の何れかとして、上記電子透かし埋込処理を行うことを特徴とする請求項１１記載の電子情報配布システム。
【請求項１９】　上記電子透かし埋込処理手段は、少なくとも上記第２のエンティティに関する情報を埋め込まない上記電子透かし埋込処理を行うことを特徴とする請求項１１又は１２に記載の電子情報配布システム。
【請求項２０】　上記原データは、画像データであるこ

とを特徴とする請求項１１記載の電子情報配布システム。

【請求項２１】　請求項１～請求項１０の何れかに記載の電子透かし方式の各工程で発生するデータを格納することを特徴とする画像ファイル装置。

【請求項２２】　請求項１～請求項１０の何れかに記載の電子透かし方式の各工程をコンピュータが読出可能に格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子透かし方式、電子情報配布システム、画像ファイル装置、及び上記電子透かし方式を実施するための工程をコンピュータが読出可能に格納した記憶媒体に関するものであり、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のディジタル情報における著作権を保護するための電子透かし方式、それを用いてディジタル情報の配布を行うマルチメディアネットワークシステム等の電子情報配布システム、上記電子透かし方式を用いた画像ファイル装置、及び上記電子透かし方式を実施するための工程をコンピュータが読出可能に格納した記憶媒体に関するものである。

【０００２】

【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。そこで取引される商品としては、例えば画像等を含むディジタルデータが考えられる。しかし、ディジタルデータは、完全なコピーを容易かつ大量に作成できるという性質を持ち、これは、そのディジタルデータを買ったユーザがオリジナルと同質のコピー（不正コピー）を不正に作成して再配布できるという可能性を示す。これにより、本来ディジタルデータの著作者又は著作者から正当に販売を委託された者（以下、「販売者」と言う）に支払われるべき代価が支払われず、著作権が侵害されていると考えられる。

【０００３】一方、著作者又は販売者（以下、上述のディジタルデータを正当に配布する者をまとめて「サーバ」と言う）がユーザにディジタルデータを一度送ってしまうと、上述の不正コピーを完全に防止することはできない。このため、不正コピーを直接防止するのではなく、「電子透かし」と呼ばれる手法が提案されている。この「電子透かし」とは、オリジナルのディジタルデータにある操作を加え、ディジタルデータに関する著作権情報やユーザに関する利用者情報をディジタルデータ中に埋め込むことによって、不正コピーが見つかった場合に誰がデータを再配布したのかを特定する手法である。

【０００４】従来の電子透かしを用いたシステムでは、サーバは完全に信頼できる機関であることが前提となっている。よって、もしサーバが信頼できる機関ではなく不正を行う可能性があるとすると、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう場合が存在する。

【０００５】これは、図１２に示すように、従来のシステムでは、ユーザを特定するための利用者情報ｄ１をディジタルデータ（以下、ディジタルデータを画像データとして説明する）ｇにサーバが埋め込むので、サーバが勝手に利用者情報ｄ１を埋め込んでそのコピーを不正に配布した場合、その利用者情報ｄ１から特定されるユーザは、サーバの主張を退ける手段がないためである。

【０００６】その対策として、例えば、「B.Pfitmann and M.Waidner：“Asymmetic Fingerprinting,”EUROCRYPT'96」の文献（以下、文献１と言う）に、公開鍵暗号方式を用いたシステム（図１３）が提案されている。

【０００７】ここで、公開鍵暗号方式とは、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。その代表例として、ＲＳＡ暗号やＥｌＧａｍａｌ暗号等が知られている。以下、公開鍵暗号方式における（ａ）特徴、（ｂ）秘密通信や認証通信等のプロトコルについて述べる。

【０００８】（ａ）公開鍵暗号の特徴

（１）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（２）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（３）送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【０００９】（ｂ）公開鍵暗号のプロトコル

例えば、通信文Ｍに対して、公開の暗号鍵ｋｐを用いて行う暗号化操作をＥ（ｋｐ，Ｍ）とし、秘密の復号鍵ｋｓを用いて行う復号操作をＤ（ｋｓ，Ｍ）とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

（１）暗号鍵ｋｐが与えられたとき、暗号化操作Ｅ（ｋｐ，Ｍ）の計算は容易である。また、復号鍵ｋｓが与えられたとき、復号操作Ｄ（ｋｓ，Ｍ）の計算は容易である。

（２）もしユーザが復号鍵ｋｓを知らないなら、暗号鍵ｋｐと、暗号化操作Ｅ（ｋｐ，Ｍ）の計算手順と、暗号文Ｃ＝Ｅ（ｋｐ，Ｍ）とを知っていても、通信文Ｍを決定することは計算量の点で困難である。

【００１０】つぎに、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより秘密通信機能が実現できる。

（３）全ての通信文（平文）Ｍに対し暗号化操作Ｅ（ｋｐ，Ｍ）が定義でき、

Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））＝Ｍ

が成立する。つまり、暗号鍵ｋｐは公開されているた

め、誰もが暗号化操作Ｅ（ｋｐ，Ｍ）の計算を行うことができるが、Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））の計算をして通信文Ｍを得ることができるのは、秘密の復号鍵ｋｓを持っている本人だけである。

【００１１】一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立することにより認証通信機能が実現できる。

（４）全ての通信文（平文）Ｍに対し復号操作Ｄ（ｋｓ，Ｍ）が定義でき、

Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ））＝Ｍ

が成立する。つまり、復号操作Ｄ（ｋｓ，Ｍ）の計算ができるのは秘密の復号鍵ｋｓを持っている本人のみであり、他の人が偽の秘密の復号鍵ｋｓ’を用いてＤ（ｋｓ’，Ｍ）の計算を行い、秘密の復号鍵ｋｓを持っている本人になりすましたとしても、

Ｅ（ｋｐ，Ｄ（ｋｓ’，Ｍ）≠Ｍ

であるため、受信者は受けとった情報が不正なものであることを確認できる。また、Ｄ（ｋｓ，Ｍ）の値が改ざんされても、

Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ）’）≠Ｍ

となり、受信者は受けとった情報が不正なものであることを確認できる。

【００１２】上述のような公開鍵暗号方式では、公開の暗号鍵（以下、公開鍵とも言う）ｋｐを用いる処理Ｅを「暗号化」、秘密の復号鍵（以下、秘密鍵とも言う）ｋｓを用いる処理Ｄを「復号」と呼んでいる。したがって、秘密通信では送信者が暗号化を行い、その後受信者が復号を行なうが、認証通信では送信者が復号を行い、その後受信者か暗号化を行うことになる。

【００１３】以下に、公開鍵暗号方式により送信者Ａから受信者Ｂへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。ここで、送信者Ａの秘密鍵をｋｓＡ、公開鍵をｋｐＡとし、受信者Ｂの秘密鍵をｋｓＢ、公開鍵をｋｐＢとする。

【００１４】〔秘密通信〕送信者Ａから受信者Ｂへ通信文（平文）Ｍを秘密通信する場合は、次の手順で行う。

Step１：送信者Ａは、受信者Ｂの公開鍵ｋｐＢで通信文Ｍを以下のように暗号化し、暗号文Ｃを受信者Ｂに送る。

Ｃ＝Ｅ（ｋｐＢ，Ｍ）

Step２：受信者Ｂは自分の秘密鍵ｋｓＢで暗号文Ｃを以下のように復号し、もとの平文Ｍを得る。

Ｍ＝Ｄ（ｋｓＢ，Ｃ）

尚、受信者Ｂの公開鍵ｋｐＢは不特定多数に公開されているので、送信者Ａに限らず全ての人が受信者Ｂに秘密通信できる。

【００１５】〔認証通信〕送信者Ａから受信者Ｂへ通信文（平文）Ｍを認証通信する場合は、次の手順で行う。

Step１：送信者Ａは、自分の秘密鍵ｋｓＡで送信文Ｓを以下のように生成し、受信者Ｂに送る。

Ｓ＝Ｄ（ｋｓＡ，Ｍ）

この送信文Ｓを「署名文」と言い、署名文Ｓを得る操作を「署名」と言う。

Step２：受信者Ｂは、送信者Ａの公開鍵ｋｐＡで署名文Ｓを以下のように復元変換し、もとの平文Ｍを得る。

Ｍ＝Ｅ（ｋｐＡ，Ｓ）

もし、通信文Ｍが意味のある文であることを確認したならば、通信文Ｍが確かに送信者Ａから送られてきたことを認証する。送信者Ａの公開鍵ｋｐＡは不特定多数に公開されているので、受信者Ｂに限らず全ての人が送信者Ａの署名文Ｓを認証できる。このような認証を「ディジタル署名」とも言う。

【００１６】〔署名付秘密通信〕送信者Ａから受信者Ｂへ通信文（平文）Ｍを署名付秘密通信する場合は、次の手順で行う。

Step１：送信者Ａは、自分の秘密鍵ｋｓＡで通信文Ｍを以下のように署名し、署名文Ｓを作る。

Ｓ＝Ｄ（ｋｓＡ，Ｍ）

さらに、送信者Ａは、受信者Ｂの公開鍵ｋｐＢで署名文Ｓを以下のように暗号化し、暗号文Ｃを受信者Ｂに送る。

Ｃ＝Ｅ（ｋｐＢ，Ｓ）

Step２：受信者Ｂは、自分の秘密鍵ｋｓＢで暗号文Ｃを以下のように復号し、署名文Ｓを得る。

Ｓ＝Ｄ（ｋｓＢ，Ｃ）

さらに、受信者Ｂは、送信者Ａの公開鍵ｋｐＡで署名文Ｓを以下のように復元変換し、もとの平文Ｍを得る。

Ｍ＝Ｅ（ｋｐＡ，Ｓ）

もし、通信文Ｍが意味のある文であることを確認したならば、通信文Ｍが確かに送信者Ａから送られてきたことを認証する。

【００１７】尚、署名付秘密通信の各Step内における関数を施す順序は、それぞれ逆転しても良い。すなわち、上述の手順では、

Step１：Ｃ＝Ｅ（ｋｐＢ，Ｄ（ｋｓＡ，Ｍ））

Step２：Ｍ＝Ｅ（ｋｐＡ，Ｄ（ｋｓＢ，Ｃ））

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Step１：Ｃ＝Ｄ（ｋｓＡ，Ｅ（ｋｐＢ，Ｍ））

Step２：Ｍ＝Ｄ（ｋｓＢ，Ｅ（ｋｐＡ，Ｃ））

【００１８】そこで、上述のような公開鍵暗号方式を適用した従来の電子透かしを用いるシステム（上記図１３）における操作の手順を示す。

【００１９】１）先ず、サーバとユーザ間で画像データｇの売買に関する契約書ｄ２を取り交わす。

【００２０】２）次に、ユーザは、自分を示す乱数ＩＤを発生させ、これを用いて一方向性関数ｆを生成する。この一方向性関数とは、関数ｙ＝ｆ（ｘ）において、ｘからｙを求めることは容易だが、逆にｙからｘを求めることが困難な関数を言う。例えば、桁数の大きな整数に

対する素因数分解や離散的対数等が一方向性関数としてよく用いられる。
３）次に、ユーザは、契約書ｄ２と一方向性関数ｆに対して、自分の秘密鍵ｋｓＵを用いて署名情報ｄ３を生成し、それらを合わせてサーバに送る。
【００２１】４）次に、サーバは、ユーザの公開鍵ｋｐＵを用いて署名情報ｄ３と契約書ｄ２を確認する。
５）サーバは確認後、現在までの全配布記録ｄ４と、ユーザが作成した乱数ＩＤとを画像データｇに埋め込み、電子透かし付き画像データ（ｇ＋ｄ４＋ＩＤ）を生成する。
６）サーバは、ユーザにその電子透かし付き画像データ（ｇ＋ｄ４＋ＩＤ）を送る。
【００２２】この後、不正コピーが発見された場合は、その不正画像データから埋め込み情報を抽出し、そこに含まれるＩＤからユーザを特定する。このとき、その不正コピーがサーバによって無断で配布されたものでないことは、以下のことを根拠として主張される。それは、ユーザを特定するＩＤはユーザ自身によって生成され、それを用いた一方向性関数値ｆにユーザの署名が付けられるので、サーバは任意のユーザに対してそのようなＩＤを生成できないということである。しかし、サーバとの間で正式に契約したユーザは自分を特定するＩＤをサーバに送るために、正式に契約したユーザへの罪の押し付けはやはり可能であり、契約していないユーザへの罪の押し付けが不可能になるだけである。
【００２３】そこで、正式に契約したユーザにも罪の押し付けが不可能になるシステム（図１４）が、「三浦，渡辺，嵩（奈良先端大）：“サーバの不正も考慮した電子透かしについて”，SCIS97-31C」の文献（以下、文献２と言う）に提案されている。これは、サーバを原画像サーバと埋め込みサーバに分割することによって実現される。ただし、このシステムでは、暗号化時及び復号時において、埋め込まれた電子透かしは壊されないとしている。以下、上記図１４のシステムにおける操作の手順を示す。
【００２４】１）先ず、ユーザが原画像サーバに画像データを、署名ｄ５を付けて要求する。
【００２５】２）原画像サーバは、その要求内容をユーザの署名ｄ５から確認し、その確認後に、要求された画像データｇを暗号化して埋め込みサーバに送る。この時、原画像サーバは、ユーザ名ｕ及び委託内容ｄ６に対する署名を付けて埋め込みサーバに送る。これと同時に、原画像サーバは、暗号化に対する復号関数ｆ’をユーザに送る。
【００２６】３）埋め込みサーバは、送られてきた暗号化画像データｇ’と、署名（ｕ＋ｄ６）とを確認し、ユーザ名ｕ及び委託内容ｄ６を基にユーザを特定する利用者情報ｄ７の作成及び埋め込みを行い、電子透かし付き暗号化画像データ（ｇ’＋ｄ７）を作成する。その後、埋め込みサーバは、その電子透かし付き暗号化画像データ（ｇ’＋ｄ７）をユーザに送る。
【００２７】４）ユーザは、原画像サーバから送られてきた復号関数ｆ’を用いて、電子透かし付き暗号化画像データ（ｇ’＋ｄ７）を電子透かし付き画像データ（ｇ＋ｄ７）へと復号する。
【００２８】この後、不正コピーが発見された場合は、原画像サーバはその不正画像データを暗号化して埋め込み情報を抽出し、それを埋め込みサーバに送る。埋め込みサーバは、この埋め込み情報からユーザを特定する。このシステムでは、原画像サーバはユーザを特定するための利用者情報ｄ７を画像データｇに埋め込んでおらず、また、埋め込みサーバは復号関数ｆ’を知らない（画像を元に戻せない）ので、正式に契約したユーザに対しても、各サーバはユーザの利用者情報ｄ７を無断で埋め込んだ画像データｇを不正配布できないことを根拠にしている。
【００２９】
【発明が解決しようとする課題】しかしながら、この図１４のシステムでは、原画像サーバと埋め込みサーバとの結託については考慮せず、埋め込みサーバとユーザとの結託も考えていない。よって、原画像サーバと埋め込みサーバとが結託した場合には、埋め込みサーバが原画像である画像データｇの暗号化画像データｇ’を持ち、ユーザが復号関数ｆ’を持つため、上述の図１３のシステムと同様にサーバの不正が可能であるし、埋め込みサーバとユーザとが結託した場合には、原画像（ｇ）の不正入手が可能である。
【００３０】また、原画像サーバは復号関数ｆ’をユーザに送るが、ユーザの復号関数ｆ’の管理が不十分であれば、埋め込みサーバはユーザと結託しなくてもユーザの不注意等から復号関数ｆ’を知ることができる可能性は大きい。
【００３１】さらに、このシステムでは、原画像サーバは埋め込み手段を有しない、或いは正しい埋め込みができないとしているが、埋め込み情報を抽出するのは原画像サーバであるので、埋め込み情報を解析すれば、原画像サーバが正しい埋め込みを行えるようになる可能性は高いと考えられる。これは、埋め込みサーバは自分の署名などを埋め込まないので、埋め込み情報と利用者情報の対応のみが埋め込みサーバの秘密であるが、データベース等を用いた埋め込み情報と利用者情報のランダムな対応ではなく、ある規則に基づいて利用者情報から埋め込み情報が作成される場合、解析される危険性は大きいからである。そして、この場合、上述の図１３のシステムと同様の不正が可能である。
【００３２】さらにまた、従来より、上述したように、ユーザとサーバからなるシステムは不完全ながら提案されてきたが、サーバが階層的に構成されたシステムでの安全性は保証されていなかった。これは、例えば、図１

５に示すように、サーバの下に複数の販売代理店１、・・・、ｍがあり、その下に各々複数のユーザ１１，・・・，１ｎ、・・・、ｍ１，・・・，ｍｎがあるといった階層型のシステム（階層型ネットワーク１）や、図１６に示すように、複数の著作者１、２、・・・、ｍ－１、ｍが属している販売代理店に、ある著作者が自分の画像データの販売を依頼し、その販売代理店が複数の著作者１、２、・・・、ｍ－１、ｍの画像データを多くのユーザ１、２、・・・、ｎに販売するといった階層型のシステム（階層型ネットワーク２）等では、データの売買を構成する要素が、上述したサーバとユーザの２者からサーバ（又は著作者）と代理店とユーザの３者に増すため、結託の問題等により２者の構成でなるシステムよりもその問題が複雑になるためである。尚、上記図１４に示したシステムは、広く考えると、サーバと代理店とユーザの３者の構成でなるシステムとも見れるが、上述の文献２に記載のシステムは、ここで言う階層的なシステムを想定したものではなく、１つのサーバの不正を防止するという観点からサーバを分割したものであり、上述したように、結託の問題も考慮されていないものである。

【００３３】そこで、本発明は、上記の欠点を除去するために成されたもので、データの売買を構成する要素が階層的であっても、データの不正配付を確実に防止する電子透かし方式、電子情報配布システム、画像ファイル装置、及び記憶媒体を提供することを目的とする。

【００３４】

【課題を解決するための手段】第１の発明は、第１のエンティティが原データに１次暗号化処理を行う第１の工程と、第２のエンティティが上記１次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行うと共に、電子透かし埋込処理を行う第２の工程と、第３のエンティティが上記電子透かし埋込処理後のデータに２次暗号化処理を行う第３の工程とを含む電子透かし方式であることを特徴とする。

【００３５】第２の発明は、上記第１の発明において、上記第１の工程は、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含むことを特徴とする。

【００３６】第３の発明は、上記第１の発明において、上記第２の工程は、上記電子透かし埋込処理の少なくとも前及び後の何れかに、３次暗号化処理を行う工程を含むことを特徴とする。

【００３７】第４の発明は、上記第１の発明において、少なくとも上記１次暗号化処理及び２次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する工程を更に含むことを特徴とする。

【００３８】第５の発明は、上記第１の発明において、認証局による証明書付き匿名公開鍵によって上記第３のエンティティの署名を検査する工程を更に含むことを特徴とする。

【００３９】第６の発明は、上記第１の発明において、上記第２のエンティティは、複数のエンティティを含むことを特徴とする。

【００４０】第７の発明は、上記第１の発明において、上記第２のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第３のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする。

【００４１】第８の発明は、上記第１の発明において、上記第１の工程は、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う工程を含み、第ｎ（ｎ≧１）のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも第ｎ＋１のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする。

【００４２】第９の発明は、上記第１又は２の発明において、上記電子透かし埋込処理は、少なくとも上記第２のエンティティに関する情報を埋め込まない処理であることを特徴とする。

【００４３】第１０の発明は、上記第１の発明において、上記原データは、画像データであることを特徴とする。

【００４４】第１１の発明は、少なくとも第１～第３のエンティティを含み、ネットワーク上でのデータの送受信を行う電子情報配布システムであって、上記第１のエンティティは、原データに１次暗号化処理を行う１次暗号化処理手段を備え、上記第２のエンティティは、上記１次暗号化処理後のデータに少なくとも管理処理及び配布処理の何れかを行う管理配布処理手段と、電子透かし埋込処理を行う電子透かし埋込処理手段とを備え、上記第３のエンティティは、上記電子透かし埋込処理後のデータに２次暗号化処理を行う２次暗号化処理手段を備える電子情報配布システムであることを特徴とする。

【００４５】第１２の発明は、上記第１１の発明において、上記第１のエンティティは、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備えることを特徴とする。

【００４６】第１３の発明は、上記第１１の発明において、上記第２のエンティティは、上記電子透かし埋込処理の少なくとも前及び後の何れかに、３次暗号化処理を行う３次暗号化処理手段を更に備えることを特徴とする。

【００４７】第１４の発明は、上記第１１の発明において、少なくとも上記１次暗号化処理及び２次暗号化処理の何れかの影響を受け、上記電子透かし埋込処理が行われたデータを配布する配布手段を更に備えることを特徴とする。

【００４８】第１５の発明は、上記第１１の発明におい

て、認証局による証明書付き匿名公開鍵によって上記第３のエンティティの署名を検査する検査手段を更に備えることを特徴とする。

【００４９】第１６の発明は、上記第１１の発明において、上記第２のエンティティは、複数のエンティティを含むことを特徴とする。

【００５０】第１７の発明は、上記第１１の発明において、上記第２のエンティティが上記電子透かし埋込処理により埋め込む情報を、少なくとも上記第３のエンティティに関する情報及び送信するデータに関する情報の何れかとしたことを特徴とする。

【００５１】第１８の発明は、上記第１１の発明において、上記第１のエンティティは、上記原データへの１次暗号化処理の少なくとも前及び後の何れかに、電子透かし埋込処理を行う電子透かし埋込処理手段を更に備え、第ｎ（ｎ≧１）のエンティティの上記電子透かし埋込処理手段は、上記電子透かし埋込処理により埋め込む情報を、少なくとも第ｎ＋１のエンティティに関する情報及び送信するデータに関する情報の何れかとして、上記電子透かし埋込処理を行うことを特徴とする。

【００５２】第１９の発明は、上記第１１又は１２の発明において、上記電子透かし埋込処理手段は、少なくとも上記第２のエンティティに関する情報を埋め込まない上記電子透かし埋込処理を行うことを特徴とする。

【００５３】第２０の発明は、上記第１１の発明において、上記原データは、画像データであることを特徴とする。

【００５４】第２１の発明は、請求項１～請求項１０の何れかに記載の電子透かし方式の各工程で発生するデータを格納する画像ファイル装置であることを特徴とする。

【００５５】第２２の発明は、請求項１～請求項１０の何れかに記載の電子透かし方式の各工程をコンピュータが読出可能に格納した記憶媒体であることを特徴とする。

【００５６】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【００５７】（第１の実施の形態）

【００５８】本発明は、例えば、上記図１５に示したような階層型のシステム（代理店が多数にあるシステム）に適用される。図１は、説明の簡単のために、上記図１５のシステムにおいて、複数の代理店のうちの任意の代理店に着目して、サーバ、代理店、及び代理店に属する複数のユーザのうちの任意のユーザの構成を簡略化して示したものである。以下、この図１を用いて、本システム１００について具体的に説明する。

【００５９】システム１００は、サーバ（又は著作者等）側の端末装置（サーバ端末装置）１０、代理店側の端末装置（代理店端末装置）４０、及びユーザ側の端末装置（ユーザ端末装置）２０を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにディジタルデータの授受を行うようになされている。

【００６０】サーバ端末装置１０は、ユーザ端末装置２０からのデータが供給される契約確認処理部１１と、例えば画像データ（ディジタルデータ）Ｇ及び代理店情報Ｍが供給される電子透かし埋込処理部１２と、電子透かし埋込処理部１２の出力が供給される１次暗号化処理部１３と、代理店端末装置４０からのデータが供給される１次復号処理部１４と、代理店端末装置４０からのデータが供給される確認処理部１５と、１次復号処理部１４の出力が供給されるハッシュ生成処理部１６とを備えている。そして、１次暗号化処理部１３及びハッシュ生成処理部１６の各出力は、代理店端末装置４０に供給されるようになされている。また、１次復号処理部１４の出力は、ハッシュ生成処理部１６に供給されると共に、代理店端末装置４０を介してユーザ端末装置２０にも供給されるようになされている。

【００６１】代理店端末装置４０は、ユーザ端末装置２０からのデータが供給される契約生成処理部４１と、契約生成処理部４１及びサーバ端末装置１０の１次暗号化処理部１３の各出力が供給される電子透かし埋込処理部４２と、電子透かし埋込処理部４２の出力が供給される３次暗号化処理部４３と、３次暗号化処理部４３の出力が供給されるハッシュ生成処理部４４と、ハッシュ生成処理部４４の出力が供給される確認処理部４５と、ユーザ端末装置２０からのデータが供給される３次復号処理部４６及び確認処理部４７と、３次復号化処理部４６の出力が供給される電子透かし埋込処理部４８とを備えている。そして、３次暗号化処理部４３の出力は、ハッシュ生成処理部４４に供給されると共に、サーバ端末装置１０の１次復号処理部１４及び確認処理部１５にも供給されるようになされている。また、確認処理部４５には、サーバ端末装置１０のハッシュ生成処理部１６の出力も供給され、確認処理部４５の出力は、ユーザ端末装置２０にも供給されるようになされている。さらに、電子透かし埋込処理部４８には、ユーザ端末装置２０からのデータも供給され、電子透かし埋込処理部４８の出力は、ユーザ端末装置２０に供給されるようになされている。

【００６２】ユーザ端末装置２０は、代理店端末装置４０の契約生成処理部４１に対してデータ供給する契約生成処理部２１と、サーバ端末装置の１次復号処理部１４からのデータが代理店端末装置４０を介して供給される２次暗号化処理部２４及び確認・署名処理部２８と、２次暗号化処理部２４の出力が供給されるハッシュ生成処理部２６と、代理店端末装置４０の電子透かし埋込処理部４８の出力が供給される２次復号処理部２７とを備えている。そして、２次暗号化処理部２４の出力は、ハッ

シュ生成処理部２６に供給されると共に、代理店端末装置４０の３次復号処理部４６及び確認処理部４７にも供給されるようになされている。また、ハッシュ生成処理部２６の出力は、代理店端末装置４０の確認処理部４７に供給されるようになされている。さらに、確認・署名処理部２８には、代理店端末装置４０の確認処理部４５の出力が供給されるようになされている。

【００６３】上述のようなシステム１００では、方式や秘密鍵等の１次暗号に関する情報はサーバだけが知る情報であり、２次暗号に関する情報はユーザだけが知る情報であり、３次暗号に関する情報は代理店だけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下、暗号化を「Ｅｉ（）」、復号を「Ｄｉ（）」で表わし、電子透かしに関する埋め込み処理を「＋」で表わすものとする。

【００６４】そこで、まず、システム１００における電子透かしに関する埋め込み処理について説明する。

【００６５】［埋め込み処理］

１）先ず、ユーザ端末装置２０において、ユーザが署名を付けて代理店に画像データを要求する。この要求データは、契約生成処理部２１により生成された情報（ユーザの署名情報）であり、以後、これを契約情報と呼ぶ。そして、代理店端末装置４０において、ユーザからの契約情報を受け、これを確認した後、画像データをサーバ側に要求する。

【００６６】２）次に、サーバ端末装置１０において、電子透かし埋込処理部１２は、代理店側から要求された画像データＧに代理店情報Ｍを埋め込む。そして、１次暗号化処理部１３は、電子透かし埋込処理部１２で代理店情報Ｍが埋め込まれた画像データ（Ｇ＋Ｍ）を１次暗号化Ｅ１して、代理店側に送信する。よって、代理店端末装置４０には、１次暗号化画像データＥ１（Ｇ＋Ｍ）の情報が送られることになる。

【００６７】３）次に、代理店端末装置４０において、契約生成処理部４１は、ユーザ側からの契約情報から利用者情報Ｕを生成する。そして、電子透かし埋込処理部４２は、契約生成処理部４１で生成された利用者情報Ｕを、サーバ側からの１次暗号化画像データＥ１（Ｇ＋Ｍ）に埋め込む。３次暗号化処理部４３は、電子透かし埋込処理部４２で利用者情報Ｕが埋め込まれた１次暗号化画像データＥ１（Ｇ＋Ｍ）＋Ｕを３次暗号化Ｅ３して、そのデータ（３次暗号化画像データ）Ｅ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ）を、サーバ側に送信する。これと同時に、ハッシュ生成処理部４４は、送信データ（３次暗号化画像データ）Ｅ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ））に対するハッシュ値Ｈ１を生成及び署名し、それらをサーバ側に送信する。よって、サーバ端末装置１０には、３次暗号化画像データＥ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ）と、ハッシュ値Ｈ１及びその署名が送られることになる。

【００６８】尚、上述のハッシュ値とは、一般にハッシュ関数ｈ()の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは、異なる値ｘ１，ｘ２に対してｈ（ｘ１）＝ｈ（ｘ２）となることである。また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは、任意のビット長のビット列をある長さのビット列に変換する関数ｈ()で、ｈ（ｘ１）＝ｈ（ｘ２）を満たす値ｘ１，ｘ２を容易に見出せないものである。このとき、任意の値ｙからｙ＝ｈ（ｘ）を満たす値ｘを容易に見出せないので、必然的にハッシュ関数は一方向性関数となる。このハッシュ関数の具体例としては、ＭＤ（Message Digest）５やＳＨＡ（Secure HashAlgorithm ）等が知られている。

【００６９】４）次に、サーバ端末装置１０において、確認処理部１５は、代理店側からのハッシュ値Ｈ１の署名と、そのハッシュ値Ｈ１の値が送信データ（３次暗号化画像データＥ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ））のハッシュ値と一致することを確認し、確認後送られてきたデータを保存する。また、１次復号処理部１４は、代理店側からの３次暗号化画像データＥ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ）の１次暗号化を復号してユーザ代理店側に送信する。これと同時に、ハッシュ生成処理部１６は、送信データ（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））に対するハッシュ値Ｈ２を生成及び署名し、それらを代理店側に送信する。よって、代理店端末装置４０には、データＥ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ２及びその署名とが送られることになる。

【００７０】５）次に、代理店端末装置４０において、確認処理部４５は、サーバ側からのハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データ（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認処理部４５は、サーバ側からのデータをそのままユーザ側に送信する。よって、ユーザ端末装置２０には、データＥ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ２及びその署名とが送られることになる。

【００７１】６）次に、ユーザ端末装置２０において、確認・署名処理部２８は、代理店側からのハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データ（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認・署名処理部２８は、ハッシュ値Ｈ２に自分の署名Ａを生成して、代理店を介してサーバ側に送信する。そして、代理店端末装置４０の確認処理部４５、及びサーバ端末装置１０のハッシュ生成処理１６は各々、ユーザ側からの署名Ａを確認し、その確認後それを保存する。

【００７２】７）次に、ユーザ端末装置２０において、２次暗号化処理部２４は、代理店側からのデータＥ３

（Ｇ＋Ｍ＋Ｄ１（Ｕ））を２次暗号化Ｅ２して、それを代理店側に送信する。これと同時に、ハッシュ生成処理部２６は、送信データ（Ｅ２（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））））に対するハッシュ値Ｈ３を生成及び署名し、それらを代理店側に送信する。また、自分の証明情報Ｓを生成して、それを代理店側に送信する。よって、代理店端末装置４０には、データＥ２（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ３及びその署名と、証明情報Ｓとが送られることになる。

【００７３】８）次に、代理店端末装置４０において、確認処理部４７は、ユーザ側からのハッシュ値Ｈ３の署名と、そのハッシュ値Ｈ３が送信データ（Ｅ２（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、３次復号処理部４６は、ユーザ側からのデータＥ２（Ｅ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））の３次暗号を復号する。そして、電子透かし埋込処理部４８は、ユーザ側からの証明情報Ｓを、３次復号処理部４６で復号して得られたデータＥ２（Ｇ＋Ｍ＋Ｄ１（Ｕ））に埋め込み、そのデータＥ２（Ｇ＋Ｍ＋Ｄ１（Ｕ））＋Ｓをユーザ側に送信する。また、ハッシュ生成処理部４９は、このデータＥ２（Ｇ＋Ｍ＋Ｄ１（Ｕ））のハッシュ値Ｈ４を生成し、そのハッシュ値Ｈ４に署名してユーザ側に送信する。よって、ユーザ端末装置２０には、データＥ２（Ｇ＋Ｍ＋Ｄ１（Ｕ））＋Ｓが送られることになる。

【００７４】９）次に、ユーザ端末装置２０において、確認処理部２９は、代理店側からのハッシュ値Ｈ４の署名を確認すると共に、このハッシュ値Ｈ４がデータＥ２（Ｇ＋Ｍ＋Ｄ１（Ｕ））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。そして、２次復号処理部２７は、代理店側からのデータＥ２（Ｇ＋Ｍ＋Ｄ１（Ｕ））＋Ｓの２次暗号を復号し、電子透かし付き画像データG_Wを取り出して出力する。この画像データG_Wは、

G_W＝Ｇ＋Ｍ＋Ｄ１（Ｕ）＋Ｄ２（Ｓ）

で表せる。これは、元の画像データＧに対して、代理店情報Ｍと、１次復号を受けた利用者情報（透かし情報）Ｕと、２次暗号の影響を受けた署名情報Ｓとが埋め込まれていることを示す。

【００７５】以上のことから、ユーザの署名情報Ｓの埋め込みは代理店側で行われるため、ユーザは基本的に不正することはできない。また、代理店は、ユーザの利用者情報Ｕ及び署名情報Ｓの埋め込みを行うが、利用者情報Ｕは、サーバのみが知る１次暗号の影響を受け、署名情報Ｓは、ユーザのみが知る２次暗号化の影響を受けるため、代理店は、Ｄ１（Ｕ＋Ｄ２（Ｓ））を直接元の画像データＧに埋め込むことはできない。このとき、不正コピー（不正画像）が発見された場合、例えば、図２に示すフローチャートに従った手順で不正ユーザの特定を行う（以下、これを検証処理と言う）。ただし、ここでは、上述の文献１、文献２と同様に、画像データは透かし情報の変形及び消去を受けないものとする。

【００７６】［検証処理］

１）先ず、サーバは、発見した不正画像データＧｗ’から代理店情報Ｍ’を抽出する（ステップＳ１０１）。このとき、代理店情報Ｍ’が抽出されなかった場合、サーバ（又は著作者等）の不正と認定する（ステップＳ１０２）。これは、代理店情報Ｍ’の埋め込みを行ったのはサーバ側であるためである。

【００７７】２）１）にて、正しい代理店情報Ｍが抽出された場合（Ｍ’＝Ｍの場合）、サーバは、検証局３０に不正画像データＧｗ’及び１次暗号化の鍵を提出し、不正画像データＧｗ’の１次暗号化（ステップＳ１０３）と利用者情報Ｕ’の抽出（ステップＳ１０４）を要求する。このとき、正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、後述する８）に進む。

【００７８】３）２）にて、正しい利用者情報Ｕ’が抽出されなかった場合、検証局３０は、サーバに対して、保存しているデータＥ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ）と、ハッシュ値Ｈ１及びその署名とを要求し、ハッシュ値Ｈ１及びその署名を確認する。その後、検証局３０は、データＥ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ）の１次暗号を復号し、そのハッシュ値を生成し、そのハッシュ値が代理店が保存しているハッシュ値Ｈ２と一致することを確認する。また、これと同時に、検証局３０は、ハッシュ値Ｈ２の署名検査も行う（ステップＳ１０５）。

【００７９】４）３）にて、検証局３０にて生成されたハッシュ値と、代理店が保存しているハッシュ値Ｈ２とが一致しなかった場合、検証局３０は、サーバの不正と認定する（ステップＳ１０６）。これは、サーバが提出した１次暗号の鍵が正しくないことを意味するからである。

【００８０】５）３）にて、検証局３０にて生成されたハッシュ値と、代理店が保存しているハッシュ値Ｈ２とが一致した場合、検証局３０は、代理店に３次暗号の鍵の提出を要求し、サーバが保存していたデータＥ３（Ｅ１（Ｇ＋Ｍ）＋Ｕ）の３次暗号を復号して利用者情報Ｕ’を抽出する（ステップＳ１０７）。

【００８１】６）５）にて、正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、検証局３０は、サーバの不正と認定する（ステップＳ１０８）。これは、利用者情報Ｕ’の埋め込み処理が正当に行われたことを意味するからである。また、５）までの検証処理によって、不正画像データＧｗ’の１次暗号が正しく、利用者情報Ｕ’が不正であることが示されたため、この不正画像データＧｗ’を生成できのは１次暗号を知るサーバのみであるからである。

【００８２】７）５）にて、正しい利用者情報Ｕ’が抽出されなかったた場合、検証局３０は、代理店の不正と認定する（ステップＳ１０９）。これは、埋め込み処理

において、正しい利用者情報Ｕ’が埋め込められなかったことを意味し、また、この利用者情報Ｕ’の埋め込みは代理店側で行われるからである。

【００８３】８）上述の２）にて、正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、検証局３０は、サーバと代理店に対して、保存されているハッシュ値Ｈ２と、ユーザによるハッシュ値Ｈ２の署名Ａ’との提出を要求し、その署名Ａ’を確認する（ステップＳ１１０）。

【００８４】９）８）にて、正しい署名Ａ’が確認されなかった場合（提出されなかった場合）、検証局３０は、サーバと代理店の結託による不正と認定する（ステップＳ１１１）。これは、サーバと代理店が結託して、任意のユーザ（利用者情報Ｕ’）を示すデータＧ＋Ｍ＋Ｄ１（Ｕ’）を偽造したことを意味するからである。

【００８５】１０）８）にて、正しい署名Ａ’が確認された場合（Ａ’＝Ａの場合）、検証局３０は、ユーザに対して、２次暗号の鍵の提出を要求し、不正画像データＧｗ’の２次暗号化を行い（ステップＳ１１２）、署名情報Ｓ’の抽出を行う（ステップＳ１１３）。

【００８６】１１）１０）にて、正しい署名情報Ｓ’が抽出された場合（Ｓ’＝Ｓの場合）、検証局３０は、ユーザの不正と認定する（ステップＳ１１４）。これは、２次暗号化して署名情報Ｓ’に戻す処理は、ユーザ側でしか行えないからである。

【００８７】１２）１０）にて、正しい署名情報Ｓ’が抽出されなかった場合、検証局３０は、ユーザに対して、保存されているデータＥ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ３及びその署名の提出を要求し、ハッシュ値Ｈ３及びその署名を確認する。その後、検証局３０は、データＥ３（Ｇ＋Ｍ＋Ｄ１（Ｕ））の２次暗号化を行うと共に、そのハッシュ値を生成し、それがハッシュ値Ｈ３と一致することを確認する。これと同時に、検証局３０は、ハッシュ値Ｈ３の署名検査も行う（ステップＳ１１５）。

【００８８】１３）１２）にて、検証局３０で生成されたハッシュ値と、ユーザが保存しているハッシュ値Ｈ３とが一致しない場合、検証局３０は、ユーザの不正と認定する（ステップＳ１１６）。これは、ユーザが提出した２次暗号の鍵が正しくないことを意味するからである。

【００８９】１４）１２）にて、検証局３０で生成されたハッシュ値と、ユーザが保存しているハッシュ値Ｈ３とが一致した場合、検証局３０は、代理店の不正と認定する（ステップＳ１１７）。これは、埋め込み処理において、代理店が正しく署名情報Ｓを埋め込まなかったことを意味するからである。

【００９０】以上のことにより、本実施の形態によれば、検証局３０は不正画像が発見されるまで必要なく、不正画像が発見される以前に不正を行うことはできない。また、上述の検証処理の手順が公知で、サーバと代理店とユーザが互いにその結果を見届け合うならば、検証局３０がなくても、状況に応じて各自の不正を特定することができる。

【００９１】（第２の実施の形態）

【００９２】本発明は、例えば、上記図１６に示したような階層型のシステム（代理店が１つのシステム）に適用される。図３は、説明の簡単のために、上記図１６のシステムにおいて、複数の著作者（又はサーバ等）代理店及び複数のユーザのうちの任意の著作者及びユーザに着目して、著作者（ここでは、サーバとして説明する）、代理店、及びユーザの構成を簡略化して示したものである。以下、この図３を用いて、本システム２００について具体的に説明する。

【００９３】システム２００は、上記図１に示したシステム１００と同様の構成としているが、次の点が異なっている。

１）サーバ端末装置１０において、電子透かし埋込処理部１２は設けられておらず、１次暗号化処理部１３に画像データＧのみが供給される。

２）代理店端末装置４０において、電子透かし埋込処理部４８の出力が供給されるハッシュ生成処理部４９が更に設けられており、このハッシュ生成処理部４９の出力は、ユーザ端末装置２０に供給される。

３）ユーザ端末装置２０において、代理店端末装置４０の電子透かし埋込処理部４８及びハッシュ生成処理部４９の各出力が供給される確認処理部２９が更に設けられている。

【００９４】上述のように、システム２００では、代理店を示す代理店情報Ｍの埋め込みを省略した構成としている。そこで、まず、システム２００における電子透かしに関する埋め込み処理について説明する。

【００９５】尚、上記図３のシステム２００において、上記図１のシステム１００と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【００９６】［埋め込み処理］

１）先ず、ユーザ端末装置２０において、ユーザが署名を付けて代理店に画像データ（契約情報）を要求する。そして、代理店端末装置４０において、ユーザからの契約情報を受け、これを確認した後、画像データをサーバ側に要求する。

【００９７】２）次に、サーバ端末装置１０において、１次暗号化処理部１３は、画像データＧを１次暗号化Ｅ１して、代理店側に送信する。よって、代理店端末装置４０には、１次暗号化画像データＥ１（Ｇ）が送られることになる。

【００９８】３）次に、代理店端末装置４０において、契約生成処理部４１は、ユーザ側からの契約情報から利用者情報Ｕを生成する。そして、電子透かし埋込処理部４２は、契約生成処理部４１で生成された利用者情報Ｕ

を、サーバ側からの１次暗号化画像データＥ１（Ｇ）に埋め込む。３次暗号化処理部４３は、電子透かし埋込処理部４２で利用者情報Ｕが埋め込まれた１次暗号化画像データＥ１（Ｇ）＋Ｕを３次暗号化Ｅ３して、そのデータ（３次暗号化画像データ）Ｅ３（Ｅ１（Ｇ）＋Ｕ）を、サーバ側に送信する。これと同時に、ハッシュ生成処理部４４は、送信データ（３次暗号化画像データ）Ｅ３（Ｅ１（Ｇ）＋Ｕ））に対するハッシュ値Ｈ１を生成及び署名し、それらをサーバ側に送信する。よって、サーバ端末装置１０には、３次暗号化画像データＥ３（Ｅ１（Ｇ）＋Ｕ）と、ハッシュ値Ｈ１及びその署名が送られることになる。

【００９９】４）次に、サーバ端末装置１０において、確認処理部１５は、代理店側からのハッシュ値Ｈ１の署名と、そのハッシュ値Ｈ１の値が送信データ（３次暗号化画像データＥ３（Ｅ１（Ｇ）＋Ｕ））のハッシュ値と一致することを確認し、確認後送られてきたデータを保存する。また、１次復号処理部１４は、代理店側からの３次暗号化画像データＥ３（Ｅ１（Ｇ）＋Ｕ）の１次暗号化を復号してユーザ代理店側に送信する。これと同時に、ハッシュ生成処理部１６は、送信データ（Ｅ３（Ｇ＋Ｄ１（Ｕ）））に対するハッシュ値Ｈ２を生成及び署名し、それらを代理店側に送信する。よって、代理店端末装置４０には、データＥ３（Ｇ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ２及びその署名とが送られることになる。

【０１００】５）次に、代理店端末装置４０において、確認処理部４５は、サーバ側からのハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データ（Ｅ３（Ｇ＋Ｄ１（Ｕ）））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認処理部４５は、サーバ側からのデータをそのままユーザ側に送信する。よって、ユーザ端末装置２０には、データＥ３（Ｇ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ２及びその署名とが送られることになる。

【０１０１】６）次に、ユーザ端末装置２０において、確認・署名処理部２８は、代理店側からのハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データ（Ｅ３（Ｇ＋Ｄ１（Ｕ）））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、確認・署名処理部２８は、ハッシュ値Ｈ２に自分の署名Ａを生成して、代理店を介してサーバ側に送信する。そして、代理店端末装置４０の確認処理部４５、及びサーバ端末装置１０のハッシュ生成処理１６は各々、ユーザ側からの署名Ａを確認し、その確認後それを保存する。

【０１０２】７）次に、ユーザ端末装置２０において、２次暗号化処理部２４は、代理店側からのデータＥ３（Ｇ＋Ｄ１（Ｕ））を２次暗号化Ｅ２して、それを代理店側に送信する。これと同時に、ハッシュ生成処理部２６は、送信データ（Ｅ２（Ｅ３（Ｇ＋Ｄ１（Ｕ）））に対するハッシュ値Ｈ３を生成及び署名し、それらを代理店側に送信する。また、自分の証明情報Ｓを生成して、それを代理店側に送信する。よって、代理店端末装置４０には、データＥ２（Ｅ３（Ｇ＋Ｄ１（Ｕ）））と、ハッシュ値Ｈ３及びその署名と、証明情報Ｓとが送られることになる。

【０１０３】８）次に、代理店端末装置４０において、確認処理部４７は、ユーザ側からのハッシュ値Ｈ３の署名と、そのハッシュ値Ｈ３が送信データ（Ｅ２（Ｅ３（Ｇ＋Ｄ１（Ｕ）））のハッシュ値と一致することを確認し、その確認後送られてきたデータを保存する。また、３次復号処理部４６は、ユーザ側からのデータＥ２（Ｅ３（Ｇ＋Ｄ１（Ｕ）））の３次暗号を復号する。そして、電子透かし埋込処理部４８は、ユーザ側からの証明情報Ｓを、３次復号処理部４６で復号して得られたデータＥ２（Ｇ＋Ｄ１（Ｕ））に埋め込み、そのデータＥ２（Ｇ＋Ｄ１（Ｕ））＋Ｓをユーザ側に送信する。よって、ユーザ端末装置２０には、データＥ２（Ｇ＋Ｄ１（Ｕ））＋Ｓが送られることになる。

【０１０４】９）次に、ユーザ端末装置２０において、２次復号処理部２７は、代理店側からのデータＥ２（Ｇ＋Ｄ１（Ｕ））＋Ｓの２次暗号を復号し、電子透かし付き画像データG_Wを取り出して出力する。この画像データG_Wは、

G_W＝Ｇ＋Ｄ１（Ｕ）＋Ｄ２（Ｓ）

で表せる。これは、元の画像データＧに対して、１次復号を受けた利用者情報（透かし情報）Ｕと、２次暗号の影響を受けた署名情報Ｓとが埋め込まれていることを示す。

【０１０５】以上のことから、ユーザの署名情報Ｓの埋め込みは代理店側で行われるため、ユーザは基本的に不正することはできない。また、代理店は、ユーザの利用者情報Ｕ及び署名情報Ｓの埋め込みを行うが、利用者情報Ｕは、サーバのみが知る１次暗号の影響を受け、署名情報Ｓは、ユーザのみが知る２次暗号化の影響を受けるため、代理店は、Ｄ１（Ｕ＋Ｄ２（Ｓ））を直接元の画像データＧに埋め込むことはできない。このとき、不正コピー（不正画像）が発見された場合、以下の手順で検証処理を行うことで、上述した代理店情報Ｍを用いずに、不正した代理店を特定できるようになされている。ただし、ここでは、上述の文献１、文献２と同様に、画像データは透かし情報の変形及び消去を受けないものとする。

【０１０６】［検証処理］

１）先ず、サーバは、検証局３０に対して、発見した不正画像データＧｗ’から１次暗号の鍵を提出し、不正画像データＧｗ’の１次暗号化と利用者情報Ｕ’の抽出を要求する。正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、後述する７）に進む。

【０１０７】２）１）にて、正しい利用者情報Ｕ’が抽

出されなかった場合、検証局３０は、サーバに対して、保存しているデータＥ３（Ｅ１（Ｇ）＋Ｕ）と、ハッシュ値Ｈ１及びその署名とを要求し、ハッシュ値Ｈ１及びその署名を確認する。その後、検証局３０は、データＥ３（Ｅ１（Ｇ）＋Ｕ）の１次暗号を復号し、そのハッシュ値を生成し、そのハッシュ値が代理店が保存しているハッシュ値Ｈ２と一致することを確認する。また、これと同時に、検証局３０は、ハッシュ値Ｈ２の署名検査も行う。

【０１０８】３）２）にて、検証局３０にて生成されたハッシュ値と、代理店が保存しているハッシュ値Ｈ２とが一致しなかった場合、検証局３０は、サーバの不正と認定する。これは、サーバが提出した１次暗号の鍵が正しくないことを意味するからである。

【０１０９】４）２）にて、検証局３０にて生成されたハッシュ値と、代理店が保存しているハッシュ値Ｈ２とが一致した場合、検証局３０は、代理店に３次暗号の鍵の提出を要求し、サーバが保存していたデータＥ３（Ｅ１（Ｇ）＋Ｕ）の３次暗号を復号して利用者情報Ｕ’を抽出する。

【０１１０】５）４）にて、正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、検証局３０は、サーバの不正と認定する。これは、利用者情報Ｕ’の埋め込み処理が正当に行われたことを意味するからである。また、４）までの検証処理によって、不正画像データＧｗ’の１次暗号が正しく、利用者情報Ｕ’が不正であることが示されたため、この不正画像データＧｗ’を生成できのは１次暗号を知るサーバのみであるからである。

【０１１１】６）４）にて、正しい利用者情報Ｕ’が抽出されなかったた場合、検証局３０は、代理店の不正と認定する。これは、埋め込み処理において、正しい利用者情報Ｕ’が埋め込められなかったことを意味し、また、この利用者情報Ｕ’の埋め込みは代理店側で行われるからである。

【０１１２】７）上述の１）にて、正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、検証局３０は、サーバと代理店に対して、保存されているハッシュ値Ｈ２と、ユーザによるハッシュ値Ｈ２の署名Ａ’との提出を要求し、その署名Ａ’を確認する。

【０１１３】８）７）にて、正しい署名Ａ’が確認されなかった場合（提出されなかった場合）、検証局３０は、サーバと代理店の結託による不正と認定する。これは、サーバと代理店が結託して、任意のユーザ（利用者情報Ｕ’）を示すデータＧ＋Ｄ１（Ｕ’）を偽造したことを意味するからである。

【０１１４】９）７）にて、正しい署名Ａ’が確認された場合（Ａ’＝Ａの場合）、検証局３０は、ユーザに対して、２次暗号の鍵の提出を要求し、不正画像データＧｗ’の２次暗号化を行い、署名情報Ｓ’の抽出を行う。

【０１１５】１０）９）にて、正しい署名情報Ｓ’が抽出された場合（Ｓ’＝Ｓの場合）、検証局３０は、ユーザの不正と認定する（ステップＳ１１４）。これは、２次暗号化して署名情報Ｓ’に戻す処理は、ユーザ側でしか行えないからである。

【０１１６】１１）９）にて、正しい署名情報Ｓ’が抽出されなかった場合、検証局３０は、ユーザに対して、保存されているデータＥ３（Ｇ＋Ｄ１（Ｕ））と、ハッシュ値Ｈ３及びその署名の提出を要求し、ハッシュ値Ｈ３及びその署名を確認する。その後、検証局３０は、データＥ３（Ｇ＋Ｄ１（Ｕ））の２次暗号化を行うと共に、そのハッシュ値を生成し、それがハッシュ値Ｈ３と一致することを確認する。これと同時に、検証局３０は、ハッシュ値Ｈ３の署名検査も行う。

【０１１７】１２）１１）にて、検証局３０で生成されたハッシュ値と、ユーザが保存しているハッシュ値Ｈ３とが一致しない場合、検証局３０は、ユーザの不正と認定する。これは、ユーザが提出した２次暗号の鍵が正しくないことを意味するからである。

【０１１８】１３）１１）にて、検証局３０で生成されたハッシュ値と、ユーザが保存しているハッシュ値Ｈ３とが一致した場合、検証局３０は、代理店の不正と認定する。これは、埋め込み処理において、代理店が正しく署名情報Ｓを埋め込まなかったことを意味するからである。

【０１１９】以上のことにより、本実施の形態によっても、検証局３０は不正画像が発見されるまで必要なく、不正画像が発見される以前に不正を行うことはできない。また、上述の検証処理の手順が公知で、サーバと代理店とユーザが互いにその結果を見届け合うならば、検証局３０がなくても、状況に応じて各自の不正を特定することができる。

【０１２０】（第３の実施の形態）

【０１２１】まず、近年において、電子現金と呼ばれるネットワーク上の通貨が実現されつつある。この電子現金は、通常の現金と同様に所有者の名前が記されないので匿名性が実現されている。もし、匿名性が実現されない場合、商品の売り手は、電子現金から誰がどの商品を購入したかという情報を知ることができ、ユーザのプライバシーが犯されることになるからである。このため、電子透かしによる著作者の著作権保護と同様に、ユーザのプライバシー保護の実現は重要である。

【０１２２】そこで、この第３の実施の形態では、購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには、電子透かしの本来の目的である不正配布者の特定が行えるようにする。これは、例えば、図４に示すようなシステム３００により実現される。

【０１２３】このシステム３００は、上記図３のシステム２００と同様の構成としているが、ユーザ端末装置２０には、認証局４０からの匿名公開鍵証明書が与えられ

る構成としている。

【０１２４】ここで、通常、署名情報を検査する公開鍵には、その正当性を証明するために認証局とよばれる機関による証明書が付されていることが多い。この認証局とは、公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成し、発行する。あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織として、VeriSignやCyberTrustという企業がよく知られている。

【０１２５】よって、上述した第２の実施の形態における埋め込み処理の１）において、代理店がユーザの契約情報を署名から確認する場合、認証局の証明書付きの公開鍵で確認することが考えられる。しかし、この証明書には通常、公開鍵の所有者の名前が記されている。よってこの場合、データの購入時におけるユーザの匿名性は実現されていないことになる。

【０１２６】これに対して、公開鍵と所有者の対応を認証局が秘密に保持すれば、公開鍵の証明書に所有者の名前を記さないこともできる。このような証明書付きの公開鍵を、以後「証明書付き匿名公開鍵」と呼ぶ。

【０１２７】そこで、ユーザは、上述した第２の実施の形態における埋め込み処理の１）において、契約情報と一緒に契約情報の署名、及び署名情報Ｓを検査する証明書付き匿名公開鍵を送れば、ユーザは購入時に自分を匿名にすることができる。よって、代理店には、利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正発見時にはその証明書付き匿名公開鍵を認証局５０に示して、その公開鍵に対応するユーザを教えてもらうことによって、ユーザを特定できる。

【０１２８】以上のことから、上述した第２の実施の形態における埋め込み処理の１）と、その検証処理の７）を以下のようにすることによって、ユーザの購入時の匿名性と不正発見時の不正者特定が実現される。

【０１２９】以下、上記図４のシステム３００における埋め込み処理、及び検証処理について具体的に説明する。

【０１３０】尚、上記図４のシステム３００において、上記図３のシステム２００と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略し、異なる部分についてのみ具体的に説明するものとする。また、埋め込み処理の１）と、その検証処理の１）以外については、上述した第２の実施の形態と同様であるため、その詳細な説明は省略する。

【０１３１】［埋め込み処理］

１’）先ず、ユーザ端末装置２０において、契約生成処理部２１は、認証局５０からの証明書付き匿名公開鍵と一緒に、画像データを要求する契約情報をその公開鍵に対応する署名を付けて代理店側に送る。代理店端末装置４０において、ユーザ側からの契約情報を証明書付き匿名公開鍵から確認し、その後、画像データをサーバ側に要求する。

【０１３２】以降、上述した第２の実施の形態における埋め込み処理の２）～９）と同様の処理を行う。

【０１３３】この場合も、ユーザは基本的に不正することはできず、また、代理店は、Ｄ１（Ｕ＋Ｄ２（Ｓ））を直接元の画像データＧに埋め込むことはできない。このとき、不正コピー（不正画像）が発見された場合、以下の検証処理を行う。

【０１３４】［検証処理］１）～６）先ず、上述した第２の実施の形態における検証処理の１）～６）と同様の処理を行う。

【０１３５】７’）上述の１）にて、正しい利用者情報Ｕ’が抽出された場合（Ｕ’＝Ｕの場合）、検証局３０は、その利用者情報Ｕ’と契約情報から得られる証明書付き匿名公開鍵を認証局５０に提出し、認証局５０に対して、その証明書付き匿名公開鍵に対応するユーザ名を要求する。また、検証局３０は、サーバと代理店に対して、保存しているハッシュ値Ｈ２及びユーザによるハッシュ値Ｈ２の署名Ａ’の提出を要求し、その署名Ａ’を確認する。

【０１３６】以降、上述した第２の実施の形態における検証処理の８）～１３）と同様の処理を行う。

【０１３７】以上のことにより、本実施の形態によっても、上述した第２の実施の形態と同様に、検証局３０は不正画像が発見されるまで必要なく、不正画像が発見される以前に不正を行うことはできない。また、上述の検証処理の手順が公知で、サーバと代理店とユーザが互いにその結果を見届け合うならば、検証局３０がなくても、状況に応じて各自の不正を特定することができる。

【０１３８】尚、第３の実施の形態では、第２の実施の形態におけるシステム２００に認証局５０を設けた構成としたが、これに限らず、第１の実施の形態におけるシステム１００に認証局５０を設けた構成としてもよい。この場合、第１の実施の形態における埋め込み処理の１）が上述の１’）となり、第１の実施の形態における検証処理の８）が上述の７’）となる。

【０１３９】上述の第１～び第３の実施の形態に示した画像データ及び透かし情報の埋め込み処理によって得られる各段階のハッシュ値を含む種々のデータは、以下のようなフォーマットで格納することができる。

【０１４０】例えば、下記の一般的な画像フォーマットでは、各段階で送付される画像データを画像データ部に格納し、それに対応するハッシュ値やその署名などを画像ヘッダ部に格納することができる。また、最終的にユ

ーザが保存しておく必要があるハッシュ値、及びその署名や２次暗号の鍵等を画像ヘッダ部に、電子透かし付き画像データを画像データ部に格納しておくことができる。

【０１４１】一方、下記に示すFlashPixTMファイルフォーマットでは、上述のようなハッシュ値やその署名を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、ハッシュ値やその署名等は、属性情報としてプロパティセットの中に格納しておくこともできる。

【０１４２】［一般的な画像フォーマットの説明］一般的な画像フォーマットは、図５に示すように、画像ファイルは画像ヘッダ部と画像データ部とに分けられる。一般的に画像ヘッダ部には、その画像ファイルから画像データを読み取るときに必要な情報や、画像の内容を説明する付帯的な情報が格納される。上記図５の例では、その画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置へのオフセット、カラーパレットの情報等の情報が格納されている。一方、画像データ部は、画像データを順次格納している部分である。このような画像フォーマットの代表的な例としては、Microsoft 社のＢＭＰフォーマットやCompuserve社のＧＩＦフォーマットなどが広く普及している。

【０１４３】［FlashPixTMファイルフォーマットの説明］以後説明するFlashPixTM（FlashPixは米国Eastman Kodak 社の登録商標）ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データ部に格納されていた画像データを、更に構造化してファイル内に格納する。この構造化した画像ファイルを、図６及び図７に示す。ファイル内の各プロパティやデータには、ＭＳ－ＤＯＳのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。上記図６及び図７において、影付き部分がストレージで、影なし部分がストリームであり、画像データや画像属性情報はストリーム部分に格納される。

【０１４４】上記図６において、画像データは異なる解像度で階層化されており、それぞれの解像度の画像をSubimageと呼び、Resolution０，１，・・・，ｎで示してある。各解像度の画像に対して、その画像データを読み出すために必要な情報がSubimage Header に、また画像データがSubimage data に格納される。

【０１４５】プロパティセットとは、属性情報をその使用目的や内容に応じて分類して定義したものであり、Summary info. Property Set、Image info. Property Set、Image Content Property Set、Extention list property Set がある。

【０１４６】［各プロパティセットの説明］Summary info. Property Setは、FlashPix特有のものではなく、Microsoft 社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。また、Comp Obj.Stream には、記録部（Strage）に関する一般的な情報が格納される。Image Content Property Setは、画像データの格納方法を記述する属性である（図８参照）。この属性には、画像データの階層数、最大解像度の画像の幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはＪＰＥＧ圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義などを記述する。Extention list property Set は、上記FlashPixの基本仕様に含まれない情報を追加する際に使用する領域である。更に、ICC Profile の部分には、ICC(International Color Consortinm) において規定される色空間変換のための変換プロファイルが記述される。

【０１４７】また、Image info. Property Setは、画像データを使用する際に利用できる下記のような様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの情報を格納する。

・ディジタルデータの取り込み方法／あるいは生成方法に関する情報
・著作権に関する情報
・画像の内容（画像中の人物、場所など）に関する情報
・撮影に使われたカメラに関する情報
・撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無など）の情報
・ディジタルカメラ特有の解像度やモザイクフィルタに関する情報
・フィルムのメーカ名、製品名、種類（ネガ／ポジ、カラー／白黒）などの情報
・オリジナルが書物や印刷物である場合の種類やサイズに関する情報
・スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報

【０１４８】上記図７のFlashPix Image View Object は、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する画像ファイルである。ビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応するために記憶しておく処理係数のセットである。この図７において、Global info.property setの部分には、ロックされている属性リストが記述されており、例えば、最大画像のインデックスや最大変更項目のインデックス、最終修正者の情報等が記述される。また、同図において、Source/Result FlashPix Image Object は、FlashPix画像データの実体であり、Source FlashPix Image Objectは必須で、Result FlashPix Image Objectはオプションである。Source FlashPix Image Objectはオリジナルの画像データを、ResultFlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像データをそれぞれ格納する。

【０１４９】また、Source/Result desc. Property Setは、上記画像データの識別のためのプロパティセットであり、画像ＩＤ、変更禁止のプロパティセット、最終更新日時等を格納する。Transform Property Setは、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【０１５０】〔画像データの取り扱いの説明〕ここでは、複数のタイルに分割された複数の解像度の画像を含む画像フォーマットを例に挙げて説明する。

【０１５１】図９に、解像度の異なる複数の画像から構成される画像ファイルの例を示す。この図９において、最大解像度の画像は列×行がＸ０×Ｙ０で構成されており、その次に解像度の大きい画像はＸ０／２×Ｙ０／２であり、それ以降順次、列・行ともに１／２ずつ縮小し、列・行ともに６４画素以下あるいは互いに等しくなるまで縮小されていく。

【０１５２】このように画像データを階層化した結果、画像の属性情報として「１つの画像ファイル中の階層数」や、それぞれの階層の画像に対して、一般的な画像フォーマットの項で説明したヘッダ情報と画像データとが必要となる（上記図５参照）。１つの画像ファイル中の階層の数や最大解像度の画像の幅、高さ、あるいはそれぞれの解像度の画像の幅、高さ、色構成、圧縮方式等に関する情報は、上記Image Content Property Set中に記述される（上記図８参照）。

【０１５３】さらに、各解像度のレイヤの画像は、図１０に示すように６４画素×６４画素でなるタイル毎に分割されている。画像の左上部から順次６４画素×６４画素のタイルに分割をすると、画像によっては右端および下端のタイルの一部に空白が生ずる場合がある。この場合は、それぞれ最右端画像または最下端画像を繰り返し挿入することで、６４画素×６４画素を構築する。

【０１５４】FlashPixTMでは、それぞれのタイル中の画像データをＪＰＥＧ圧縮、シングルカラー、非圧縮のいずれかの方法で格納する。ＪＰＥＧ圧縮は、ISO/IEC JTC1/SC29 により国際標準化された画像圧縮方式であり、方式自体の説明はここでは割愛する。また、シングルカラーとは、上記１つのタイルがすべて同じ色て構成されている場合にのみ、個々の画素の値を記録することなく、そのタイルの色を１色で表現する方式である。この方法は特に、コンピュータグラフィックスにより生成された画像で有効である。

【０１５５】このようにタイル分割された画像データは、例えば上記図６のSubimage dataストリーム中に格納され、タイルの総数、個々のタイルのサイズ、データの開始位置、圧縮方法はすべてSubimage Header に格納されている（図１１参照）。

【０１５６】尚、以上に述べた第１～第３の実施の形態において、透かし情報の埋め込みは、種々の手法によって実現できるが、例えば、「清水，沼尾，森本（日本ＩＢＭ）：“ピクセルブロックによる静止画像データハイディング”，情報処理学会第５３回全国大会，1N-11，平成８年９月」の文献３や、「I.J.Cox, J.Kilian, T.Leighton and T.shamoon(ＮＥＣ)：“Sucure Spread Spectrum Watermarkingfor Multimedia,”ＮＥＣ Reserch Institure Technical Report 95-10.」の文献４に示されるような公知の埋め込み手法によって実現できる。

【０１５７】また、１次暗号～３次暗号として用いられる暗号方式も種々の方式によって実現できるが、例えばビットの配置を暗号鍵に応じて換えるといった暗号方式によって実現できる。

【０１５８】さらに、全ての送信データにハッシュ値とその署名を付けて送ることもできる。

【０１５９】また、１次暗号～３次暗号は、透かし情報の埋め込み処理において互いの情報を知らせないために用いられるが、第三者からの通信路上での盗聴および改ざんを防ぐために、別にＤＥＳ（Data Encryption Standard）等の暗号やハッシュ関数等を用いても良い。

【０１６０】また、上述の第１～第３の実施の形態において、不正配布の検出はサーバ（又は著作者等）側で行っているが、１次暗号又は２次暗号に関する秘密鍵を知らなくても電子透かしの抽出手段さえ持っていれば、誰にでも不正配布および不正配布の利用者情報を知ることができる。その後、不正配布発見をサーバ側に知らせて検証処理を始めさせれば良いので、不正配布の発見者はサーバに限定されない。

【０１６１】また、サーバ側は、利用者情報Ｕだけでなく、必要に応じて著作権情報やその画像データの配布状況に関する情報等の他の情報を画像データに埋め込むこともできる。また、サーバ又は代理店側で秘密の情報を埋め込みたい場合は、１次暗号化の後に埋め込み処理を行えば、署名情報と同様に１次暗号の影響を受けた情報を埋め込むことができる。さらに、利用者情報Ｕは、必ず１次暗号化の前にある必要はなく、１次暗号化の後に埋め込んでもよい（この場合、利用者情報Ｕの検出は、サーバ又は代理店又は１次暗号の秘密鍵を知る者のみが行える）。

【０１６２】また、ユーザ側が共通のプリンタや端末等を用いる第２のエンティティである場合、ユーザの署名情報及び２次暗号は、プリンタや共通端末の署名情報や暗号方式を含む場合がある。

【０１６３】また、サーバ（又は著作者等）側の１次暗号化情報は、ユーザ側からの契約情報による依頼がなくても、ネットワークやＣＤ－ＲＯＭ等によって広く配布されていても良い。

【０１６４】また、ユーザの署名情報Ｓは、公開鍵暗号方式によって生成されるものに限らず、ユーザが契約情報等で定めた情報（暗号番号のような情報等）でもよい。

【0165】また、米国では、40ビット以上の暗号を用いる場合、暗号の悪用を防ぐために、暗号鍵を管理する鍵管理局を必要する。このような場合、検証局30に鍵管理局を兼ねさせることも可能である。よって、検証局30が2次暗号の鍵を予め管理している場合は、不正画像の監視も検証局が行うようにすれば、上述の検証処理1）～3）は検証局30が単独で行うことができる。このとき、サーバの1次暗号の鍵は、同じ検証局によって管理されていてもよいし、異なる他の検証局に管理されていてもよい。また、サーバやユーザの鍵は、鍵管理局が生成し、配付するようにしてもよい。

【0166】また、代理店は、1つは限らず、複数の代理店が階層的に構成されていてもよい。この場合、代理店の行う処理は、階層中の担当代理店が代表して行うようにしてもよいし、代理店間で上述のプロトコルを実行し、責任を明らかにするようにしてもよい。

【0167】また、サーバ（又は著作者等）は、要求された後に元の画像データGの1次暗号のデータE1（G）又はE1（G+M）を代理店側に送るようにしたが、予めデータE1（G）又はE1（G+M）を代理店側に送るようにしてもよい。

【0168】また、代理店の3次暗号の影響は、最終的に得られる画像データG_Wに残らないが、利用者情報Uの埋め込みを3次暗号化の後に行う、或いは、署名情報Sの埋め込みを3次暗号化の後に行う等をすることで、3次暗号の影響を残すようにしてもよい。

【0169】また、本発明の目的は、上述した第1～第3の実施の形態のホスト及び端末の機能を実現するための工程をソフトウェアのプログラムコードとして記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はCPUやMPU）が記憶媒体に格納されたプログラムコードを読みだして実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が上述した実施の形態の機能を実現することとなり、そのプログラムコードを記憶した記憶媒体は本発明を構成することとなる。

【0170】プログラムコードを供給するための記憶媒体としては、ROM、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD－ROM、CD－R、磁気テープ、不揮発性のメモリカード等を用いることができる。

【0171】また、コンピュータが読みだしたプログラムコードを実行することにより、上述した第1～第3の実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOS等が実際の処理の一部又は全部を行い、その処理によって第1～第3の実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0172】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部又は全部を行い、その処理によって上述した第1～第3の実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0173】

【発明の効果】以上説明したように本発明によれば、第3のエンティティ（ユーザ）に関する情報の埋め込みを第2のエンティティ（代理店等）側で行なうことができる。この場合、第3のエンティティは不正することはできない。また、第2のエンティティは、第3のエンティティに関する情報（利用者情報Uや署名情報S等）の埋め込みを行うが、その情報は、第1のエンティティ（サーバ又は著作者等）のみが知る暗号（1次暗号化、第1の暗号化手段における暗号）や、第3のエンティティのみが知る暗号（2次暗号化、第2の暗号化手段における暗号）の影響を受けるため、第2のエンティティは、第3のエンティティに関する情報を直接原データに埋め込むことはできない。したがって、階層的に構成されたネットワークにおいても、データの不正配付を確実に防止することができ、安全なシステムが実現できる。また、ユーザの匿名性も容易に実現できる。

【図面の簡単な説明】

【図1】第1の実施の形態において、本発明を適用したシステムの構成を示すブロック図である。

【図2】上記システムでの検証処理を説明するためのフローチャートである。

【図3】第2の実施の形態において、本発明を適用したシステムの構成を示すブロック図である。

【図4】第3の実施の形態において、本発明を適用したシステムの構成を示すブロック図である。

【図5】一般的な画像フォーマットを説明するための図である。

【図6】構造化画像ファイル（1）を説明するための図である。

【図7】構造化画像ファイル（2）を説明するための図である。

【図8】画像データの格納方法を記述する属性を説明するための図である。

【図9】解像度の異なる複数の画像から構成される画像ファイルの一例を説明するための図である。

【図10】各解像度のレイヤの画像を説明するための図である。

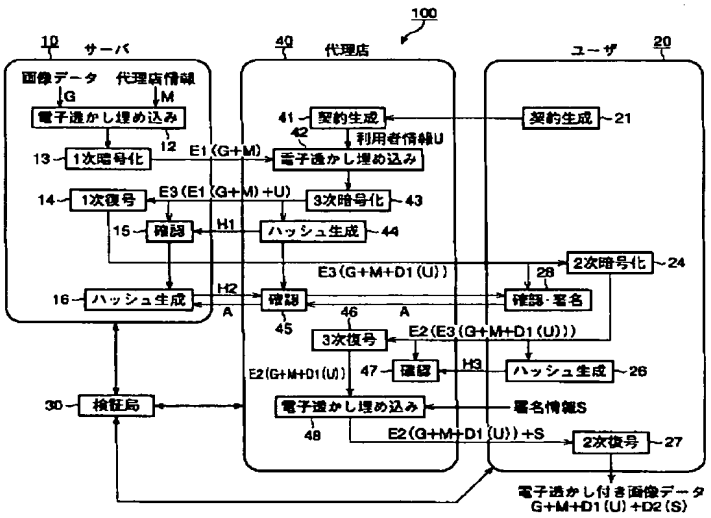
【図11】画像データの個々のタイルデータを説明するための図である。

【図12】従来の電子透かしを用いたシステムを説明するための図である。

【図13】上記システムを改良した従来の電子透かしを

用いたシステム（１）を説明するための図である。
【図１４】上記システムを改良した従来の電子透かしを用いたシステム（２）を説明するための図である。
【図１５】従来の電子透かしを用いた階層的システム（サーバ、代理店、ユーザからなるシステム）を説明するための図である。
【図１６】従来の電子透かしを用いた階層的システム（著作者、代理店、ユーザからなるシステム）を説明するための図である。
【符号の説明】
１００　電子透かしを用いたシステム
１０　サーバ側の端末装置
１２　電子透かし埋込処理部
１３　１次暗号化処理部
１４　１次復号処理部
１５　確認処理部
１６　ハッシュ生成処理部
２０　ユーザ側の端末装置
２１　契約生成処理部
２４　２次暗号化処理部
２６　ハッシュ生成処理部
２７　２次復号処理部
２８　確認・署名処理部
３０　検証局
４０　代理店側の端末装置
４１　契約生成処理部
４２　電子透かし埋込処理部
４３　３次暗号化処理部
４４　ハッシュ生成処理部
４５　確認処理部
４６　３次復号処理部
４７　確認処理部
４８　電子透かし埋込処理部

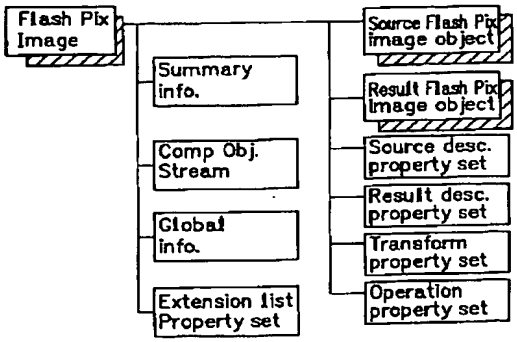
【図１】



【図５】

画像ヘッダ部	画像フォーマット識別子
	ファイルサイズ
	X方向ピクセル数（幅）
	Y方向ピクセル数（高さ）
	深さ方向サイズ
	圧縮の有無
	解像度
	ビットマップへのオフセット
	カラーパレットサイズ
画像データ部	ビットマップ

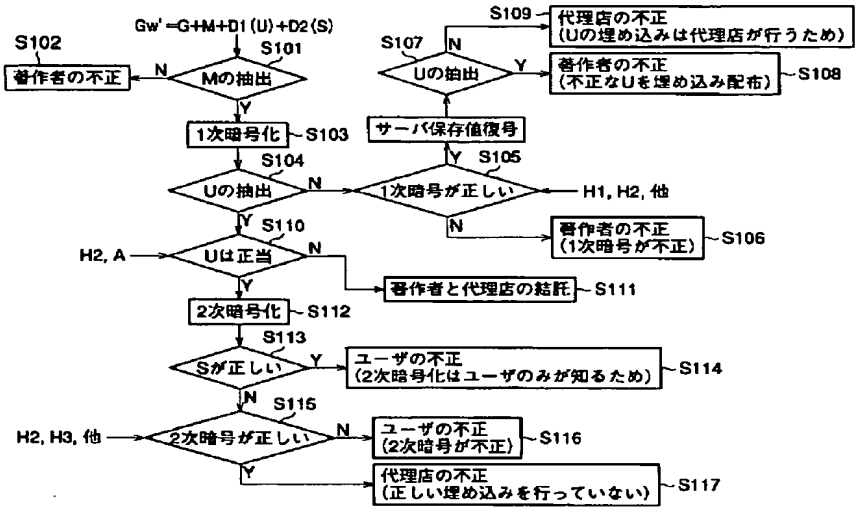
【図７】



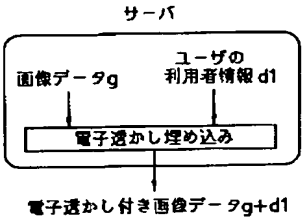
【図１１】

フィールド名	長さ	バイト
画像の幅	4	4–7
画像の高さ	4	8–11
タイルの総数	4	12–15
タイルの幅	4	16–19
タイルの高さ	4	20–23

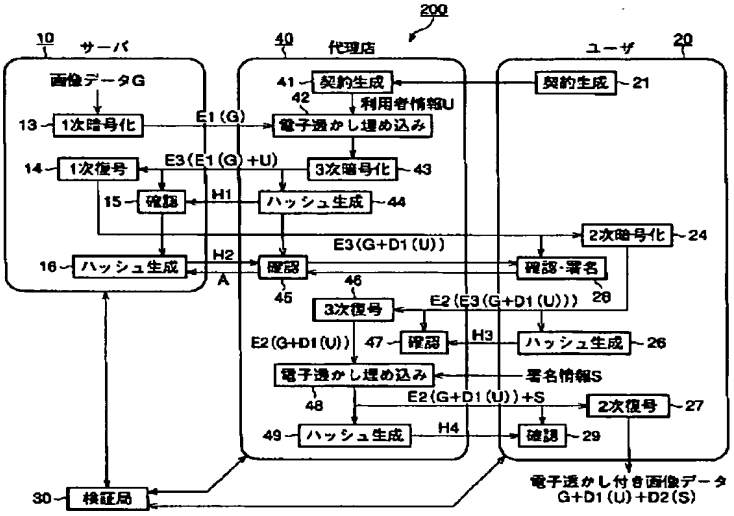
【図２】



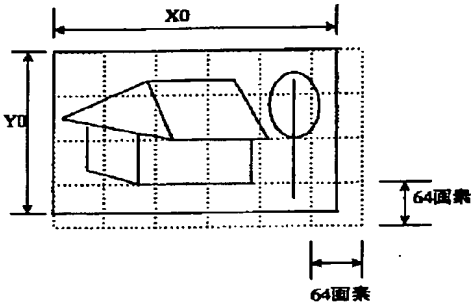
【図１２】



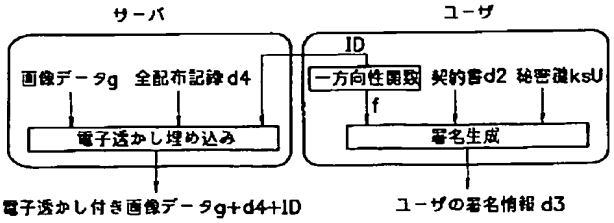
【図３】



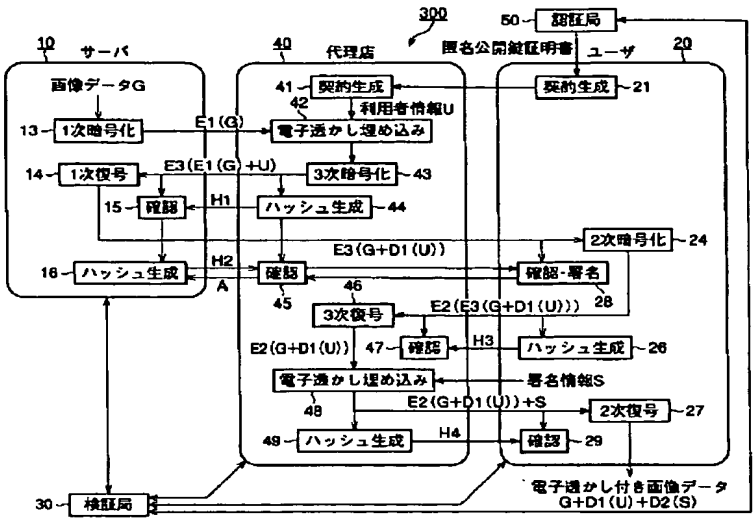
【図１０】



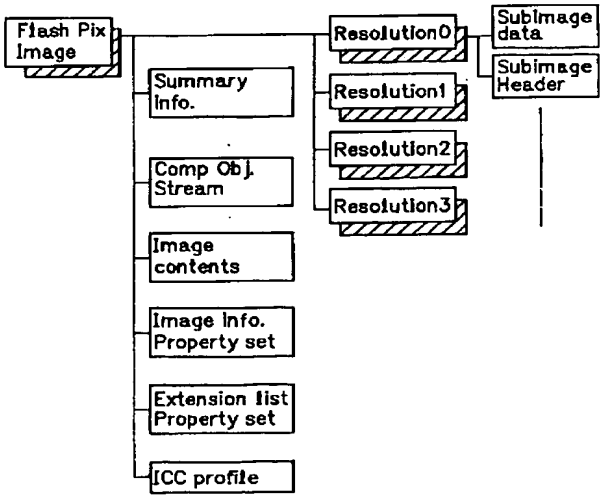
【図１３】



【図4】



【図6】



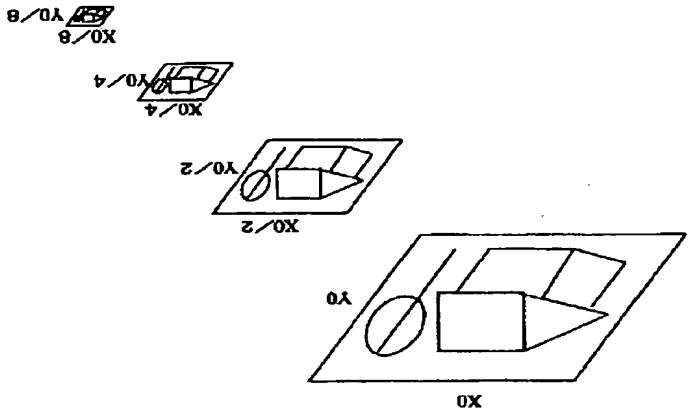
【図8】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

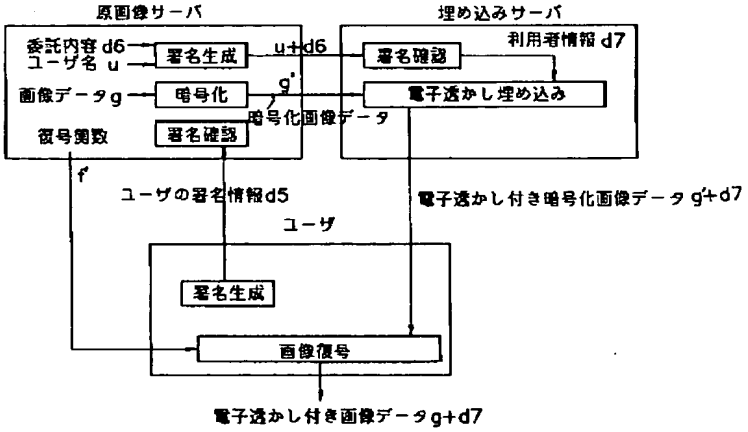
プロパティ名	IDコード	タイプ
各階像度の画像の幅	0x02ii0000	VT_UI4
各階像度の画像の高さ	0x02ii0001	VT_UI4
各階像度の画像の色	0x02ii0002	VT_BLOB
各階像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4|VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4

【図９】

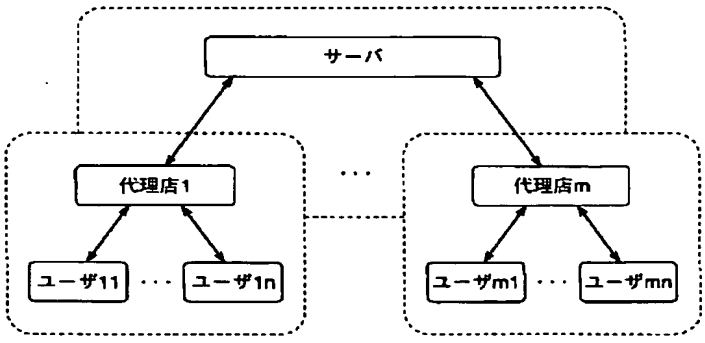


【図１４】



【図１５】

・階層型ネットワーク（１）



【図１６】

・階層型ネットワーク（２）